Adjudication

Screening (pre)

Reinvestigation

Personnel Security

Background Investigation

Possible for

the Glossary -

STAT per

Declassified in Part - Sanitized Copy Approved for Release
2013/04/15 : CIA-RDP91B00390R000500590031-7

28 July 1988

25X1 MEMORANDUM FOR: [redacted]
Chief, Policy Branch/PPS/OS

25X1 FROM: [redacted]
Policy Branch/PTS

SUBJECT: PTS Proposed Changes to the "Glossary of Intelligence Terms and Definitions"

1. The attached document is a suggested list of changes to subject glossary. The listing is unclassified.

2. During the course of review and discussion of the glossary, it was also suggested that the definition for "personnel security" was inaccurate and more closely defines "background investigation," which was noted to be missing. The official definitions for both would more appropriately be provided by the Personnel Security experts.

25X1 3. Please feel free to contact me with any questions on these proposed changes. [redacted]

C O N F I D E N T I A L

ADDITIONS:

Accreditation: An official management authorization to operate an Automated Information System or network in a particular security mode of operation, with a prescribed set of administrative, environmental, and technical safeguards, against a defined threat, in a given operational environment, under a stated operational concept, with stated interconnections to other systems or networks at an acceptable level of risk.

Accrediting Authority: A US Government Official with Intelligence authorities and responsibilities identified in Executive Order 12333, who approves Automated Information Systems processing intelligence information for operation.

Acceptable Level of Risk: An assessment by an appropriate accrediting authority that the value of an Automated Information System unambiguously outweighs the likelihood of potential damage to the security interests of the United States in the event information from the system is compromised, damaged, or destroyed.

Automated Information Systems (AIS): An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information. It will typically consist of automatic data processing (ADP) system hardware, operating system and applications software, associated peripheral devices, and associated data.

CAP (Countermeasures Advisory Panel): - An interagency panel which recommends National TEMPEST policy for approval by the National Telecommunications and Information Systems Security Committee (NTISSC)

CE (Counterespionage) -- Add CE to Appendix A (Acronyms and Abbreviations).

Certification: A comprehensive evaluation made as part of the accreditation process that establishes the extent to which a specified set of requirements are met.

Communications Security: The protection resulting from the application of cryptosecurity, transmission security, and emission security measures to telecommunications and from the application of physical security measures to communications security information.

Compartmented Mode of Operation: A security yardstick which is achieved when all users of an information system have National Intelligence Clearance, but have not signed non-disclosure agreements, for all information on the system.

Countermeasures: Defensive techniques designed to detect, prevent or expose the use of electronic audio or visual surveillance devices. Sweeping.

Covert Communications (COVCOM): An assumably of clandestine communications equipment, techniques, and operational tradecraft used in the transmission of messages by agents operating within denied areas. COVCOM generally implies undetected transmissions by radio, by long and short range.

Dedicated Mode of Operation: A security yardstick which is achieved when all users of an information system have National Intelligence Clearance, have signed non-disclosure agreements, and have need-to-know for all information in the system.

Destruction Device: U.S. Government approved equipment for the terminal destruction of classified material as required by intelligence community standards.

Detection: Describes a technical process wherein proscribed thresholds or specific conditions have been met with an expected indication of this condition is manifest. Examples of each would be that a radio signal is strong enough to be displayed on the receiver, and that an alarm system has sensed the movement of an intruder and sounded the bell. In general usage, the word detection implies both that the indication exists and that it is recognized and properly interpreted.

E-Field: Electric field signals; signal strength drops off slowly (proportional to the inverse square of the distance).

Emanations Security: The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising signals from other than crypto-equipment and telecommunications systems.

Emission Security: That component of communications security which results from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

Field Review: A review of all security features associated with a system in its operational environment to insure that minimum policy requirements are addressed. A field review is performed as part of the accreditation process.

H-Field: Magnetic field signals; signal strength drops off quickly (proportional to the inverse cube of the distance).

Implant: An electronic device or component modification to electronic equipment which is designed to gain unauthorized interception of information-bearing energy via technical means.

Indirect Automated Information System User: A customer (q.v.) who receives system output produced outside of his control. Indirect users of Automated Information Systems must be included in determining the mode of operation of an automated information system for the accreditation process.

Information System Security Officer: An individual formally appointed by an accrediting authority to ensure that the provisions of all applicable directives are implemented throughout the life cycle of each automated information system.

Intrusion Detection Systems (IDS): A security alarm system consisting of various types of components (balanced magnetic switches, capacitance, infrared, ultrasonic, etc.) to detect intrusion in the area of coverage within a facility.

Line-of-sight: The accessibility of a physical target in a direct or uninterrupted visual path to a distant surveillance point.

Multi-level Mode of Operation: A security yardstick which is attained when some users of an information system do not have a National Intelligence Clearance for access to some information in a system.

National Intelligence Clearance: A clearance for access to intelligence information granted by an authorized authority under the provisions of Director of Central Intelligence Directive 1/14.

National Telecommunications and Information Systems Security Committee (NTISSC): Interagency committee with responsibility-ties to approve national security policies for TEMPEST and telecommunications security.

Plain Text Processing Equipment (PTPE): Equipment used to process classified information in plain text (unencrypted) form. Included are manual, electric and electronic typewriters; photocopiers, computer equipment; audio/visual equipment; and microfiche readers and printers.

Safehaven: (1) a protected or reinforced area within an official facility or personal residence located overseas to which occupants can retreat during an emergency and remain until the situation returns to normal or outside help arrives;

(2) a foreign country or a protected area within a foreign country affording a hiding place or temporary asylum for persons evading hostile government elements.

Safekeeping Equipment: U.S. Government approved containers for the storage and protection of classified information as required by intelligence community standards.

Security Mode of Operation of an Automated Information System: A security yardstick which indicates the relative level of risk to information in an automated information system. There are four modes of operation: dedicated, system high, compartmented, and multi-level. The mode of operation is defined as a comparison between information sensitivity and user trust.

Security Survey: A comprehensive formal evaluation of a facility, area, or activity by security specialists to determine its physical or technical strengths and weaknesses and to propose recommendations for improvement.

Secure Telephone: (Defer to OC, OIT, or OS/TSD for appropriate official definition. The item is used throughout the IC.

SIG-I -- Senior Interagency Group - Intelligence -- "The SIG-I is 'the principal forum where the national perspective can be brought to counterintelligence (CI) and countermeasures (CM) policy,'..."[1] Three interagency groups (IG's) are subordinate to the SIG-I, the Interagency Group/Counterintelligence (IG/CI), the Interagency Group/Countermeasures (Technical) [IG/CM(T)] and the Interagency Group/Countermeasures (Policy) [IG/CM(P)]. "The IG/CI deals in counterintelligence policy. The IG/CM(T) deals in technical matters and the IG/CM(P) non-technical issues. The IG/CM(T) is headed by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, is intended in part to serve as a bridge between the intelligence world of the SIG-I and the world of the National Telecommunications and Information Systems Security Committee (NTISSC)."[2]

1. Meeting the Espionage Challenge: A Review of United States Counter Intelligence and Security Programs, Report #99-522, 1986, Report of the Select Committee on Intelligence United States Senate

2. Ibid.

Survey: (See Security Survey)

Sweep: (See Countermeasures)

Technical Penetration: A deliberate penetration of a secure area by technical means to gain unauthorized interception of information-bearing energy.

Technical Surveillance Countermeasures (TSCM): Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies which are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluidic and acoustic means, as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information meant to be protected. TSCM also includes the development and use of protective systems to detect and deter hostile penetration attempts and the hostile exploitation of naturally occurring hazards. TSCM measures include detection and neutralization of hostile penetration efforts against telephones and telephone systems, secure conference rooms and office areas, and equipment for storage and handling of classified information.

Technical Surveillance Hazard: A condition which could permit the technical penetration of an area wherein sensitive information might be compromised. A hazard may be caused by equipment, which by reasons of its normal design and installation, or by reasons of faulty fabrication, installation, operation or maintenance, or by reasons of accidental damage, could facilitate the unintentional transmission of sensitive information. Technical surveillance hazards are not necessarily limited to inherent characteristics or accidental malfunctions of various equipments, but may be caused by furnishings or even structural members.

Technical Surveillance Countermeasures (TSCM) Monitor: A limited TSCM inspection, normally provided in conjunction with sensitive briefings, conferences, and seminars, which consists basically of an examination of portions of the electromagnetic spectrum and a thorough physical and visual examination of the area.

Technical Surveillance Device: A device covertly installed to monitor (visually, audibly, or electronically) sensitive activities and/or information processing within a target area.

Zone of Control: Spherical zone around a piece of equipment not permitted access by unauthorized personnel without escort.

4 C: Community-wide, Computer Assisted, Compartmented, Control System. (Addition to Appendix A - Acronyms and Abbreviations).

CHANGES

"Automated data processing system security" to "Automated Information System Security;" as well as the phrase "needed to provide an acceptable level of protection" to "needed to operate with an acceptable level of risk."

Computer Security: Technical, administrative, and programmatic means by which assurance can be gained of correct, timely, and accountable delivery of appropriate information to authorized customers through automation. Alternatively, the technical, administrative, and programmatic means by which incorrect, untimely, unaccountable, or inappropriate delivery of information can be countered.

Rationale: Computer security is about accountability and correctness not about mechanisms and techniques --- the definition being replaced is fundamentally incorrect.

Information Security: Safeguarding information against unauthorized disclosure, modification, destruction, or denial of rightful access; and the technical, and administrative means by which individual accountability for information access, dissemination, and destruction is achieved throughout the information life cycle.

Rationale: The definition as given in the current Glossary is incomplete. Individual accountability, destruction, modification, and the denial of access are fundamental parameters of information security. Information security must be exercised throughout the information life cycle from creation to destruction.

DELETIONS

Multi-level Security

Rationale: Definition is internally inconsistent. Modes of operation (e.g., Dedicated Mode, System High Mode, Compartmented Mode, and Multi-level Mode) replace this term.

Uni-level Security

Rationale: Same as above.

The following phrase from paragraph headed:
"CAUTION-PROPRIETARY INFORMATION INVOLVED (PROPIN)"

"...that has any interest, actual or potential, in competition with the source of the information"...